Zone Mismatch Handling

The Zone Mismatch Handling feature allows you to validate the zone pair that is associated with an existing session and allows traffic that matches the zone pair into the network. Allowing traffic into the network without validating the zone pair associated with a session can lead to security vulnerabilities.

This module provides an overview of the feature and explains how to configure it.

- Finding Feature Information, on page 1
- Restrictions for Zone Mismatch Handling, on page 1
- Information About Zone Mismatch Handling, on page 2
- How to Configure Zone Mismatch Handling, on page 3
- Configuration Examples for Zone Mismatch Handling, on page 4
- Additional References for Zone Mismatch Handling, on page 5
- Feature Information for Zone Mismatch Handling, on page 6

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Zone Mismatch Handling

You cannot configure the **zone-mismatch drop** command under the **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, and **parameter-map type inspect global** commands.

Information About Zone Mismatch Handling

Zone Mismatch Handling Overview

The zone-based firewall creates sessions for traffic that flows from a source zone to a destination zone, and also matches the traffic when it returns from the destination zone to the source zone. A zone is a group of interfaces that have similar functions or features. A zone pair allows you to specify a unidirectional firewall policy between two security zones that are part of a zone pair.

For the first packet of the traffic, the firewall checks the zone pair that is associated with the ingress and egress interfaces of the packet, and validates the packet before it creates a session for traffic that can be inspected. And when the return traffic comes, the firewall does a session lookup based on the first packet to find an existing session. If the firewall finds a matching session, it allows the traffic to passthrough, and does not check whether the zone associated with the return traffic matches with the zone pair associated with the existing session. Allowing traffic into the network without validating the zone-pair associated with a session can lead to security vulnerabilities.

The Zone Mismatch Handling feature allows you to validate the zone pair that is associated with an existing session and allows traffic that matches the zone pair into the network. When you configure the **zone-mismatch drop** command, the firewall drops all packets (IPv4 and IPv6) that match an existing session but whose zone pair does not match the zone through which these packets arrive or leave. This feature works along with high availability and In-Service Software Upgrade (ISSU).

When you configure the **zone-mismatch drop** command under the **parameter-map type inspect-global** command, the zone mismatch handling configuration applies to the global firewall configuration. Traffic between all zones are inspected for zone-pair mismatch.

You can also configure the **zone-mismatch drop** command under the **parameter-map type inspect** command. This allows you to apply the Zone-Mismatch Handling feature on a per-policy basis.

When you configure the **zone-mismatch drop** command, the configuration is effective only for new sessions. For existing sessions, traffic is not dropped if the sessions do not belong to the same zone-pair.

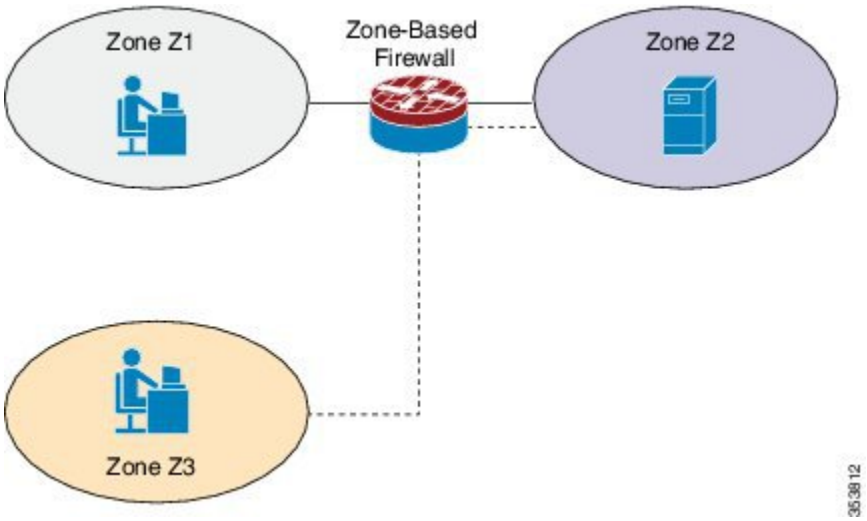
Deployment Scenarios for Zone Mismatch Handling

This section describes some typical scenarios in which the Zone Mismatch Handling feature is deployed:

Traffic Inspection by the Zone-Based Firewall

The following illustration shows traffic inspection by the firewall when the Zone Mismatch Handling feature is enabled.

Figure 1: Traffic Inspection by the Zone-Based Firewall



Zones Z1 and Z2 are part of the same zone pair, which has a parameter map that has the **zone-mismatch drop** command configured on it. Because zone Z3 is not part of the zone pair, the traffic from Z3 is dropped even if the traffic matches the firewall sessions between interface 1 and interface 2.

If you configure the **zone-mismatch drop** command for the parameter-map that is associated with the zone pair to which zone Z3 is attached, that configuration will not be effective for sessions established between Z1 and Z2. However, if you configure the **zone-mismatch drop** command under the **parameter-map type inspect-global** command, the configuration is effective for traffic between all the zones.

Application Layer Gateways Configured with the Zone-Based Firewall

Some application layer gateways (ALGs) also called application-level gateways require multiple control and media channels to operate. The zone-based firewall does not enforce that control and media channels should be in the same zone pair for ALGs. When you configure the **zone-mismatch drop** command for media or data channels, the configuration takes effect after the media or data channels are promoted from imprecise to precise sessions. The zone-based firewall checks these precise sessions like normal sessions. Imprecise sessions are sessions that do not have all 5-tuple information.

How to Configure Zone Mismatch Handling

Configuring Zone Mismatch Handling

You cannot configure the zone-mismatch drop command under the **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, and **parameter-map type inspect global** commands.

If you configure the **zone-mismatch drop** command under the **parameter-map type inspect-global**command, the zone mismatch handling configuration applies to the global firewall configuration.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. Do one of the following:
   - **parameter-map type inspect** *parameter-map-name*
   - **parameter-map type inspect-global**
4. **zone-mismatch drop**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables user EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Do one of the following:
	• **parameter-map type inspect** *parameter-map-name*
	• **parameter-map type inspect-global**
	Example:
	`Device(config)# parameter-map type inspect pmap1`
	`or`
	`Device(config)# parameter-map type inspect-global`
		Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action and enters parameter-map type inspect configuration mode.

Step 4	**zone-mismatch drop** **Example:** `Device(config-profile)# zone-mismatch drop`	Validates the zone pair that is attached to an existing session and allows traffic that matches the zone pair into the network. If the zone pair of an incoming session does not match the zone through which the session arrives or leaves, the firewall drops these packets.
Step 5	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Configuration Examples for Zone Mismatch Handling

Example: Configuring Zone Mismatch Handling

In the following example, the Zone Mismatch Handling feature is enabled for parameter map pmap-fw.

```
! Configuring zones
Device(config)# zone security private
Device(config-sec-zone)# exit
```

```
Device(config)# zone security public
Device(config-sec-zone)# exit
Device(config)# zone security internet
Device(config-sec-zone)# exit

! Attaching zones to interfaces
Device(config)# interface GigabitEthernet 0/1/5
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# zone-member security private
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# ip address 209.165.200.226 255.255.255.0
Device(config-if)# zone-member security public
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/1/1
Device(config-if)# ip address 198.51.100.1 255.255.255.0
Device(config-if)# zone-member security internet
Device(config-if)# no shutdown
Device(config-if)# exit

!Configuring the Zone Mismatch Handling feature
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# zone-mismatch drop
Device(config-profile)# exit

!Configuring class maps
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit

! Configuring policy maps and class matching
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit

! Configuring zone pairs
Device(config)# zone-pair security private-internet source private destination internet
Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy
Device(config-sec-zone-pair)# end
```

Additional References for Zone Mismatch Handling

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security Commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Zone Mismatch Handling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Zone Mismatch Handling

Feature Name	Releases	Feature Information
Zone Mismatch Handling	Cisco IOS XE 3.15S	The Zone Mismatch Handling feature allows you to validate the zone-pair associated with an existing session and allows traffic that matches the zone-pair into the network. This feature is supported on Cisco 4400 Series Integrated Services Routers,Cisco ASR 1000 Series Aggregation Services Routers, and Cisco Cloud Services Router 1000V Series. The following command was introduced: **zone-mismatch handling**.